Optically programmable logic cells as basic units for transmission and synchronization of chaotic signals

A. Gonzalez-Marcos*, J.A. Martin-Pereda
E.T.S. Ingenieros de Telecomunicación. Universidad Politécnica de Madrid

ABSTRACT

We proposed an optical communications system, based on a digital chaotic signal where the synchronization of chaos was the main objective, in some previous papers. In this paper we will extend this work. A way to add the digital data signal to be transmitted onto the chaotic signal and its correct reception, is the main objective. We report some methods to study the main characteristics of the resulting signal. The main problem with any real system is the presence of some retard between the times than the signal is generated at the emitter at the time when this signal is received. Any system using chaotic signals as a method to encrypt need to have the same characteristics in emitter and receiver. It is because that, this control of time is needed. A method to control, in real time the chaotic signals, is reported.

Keywords: Chaos synchronization, digital chaos, encryption.

1. INTRODUCTION

A considerable interest has appeared in the last years concerning the application of chaotic circuits in order to obtain secure communications. The broadband nature of chaotic signals makes them tempting for use in this area and in spread-spectrum situations. The fact that such signals emanate from a deterministic dynamic system lends to the hope that one will also be able to control them sufficiently for many uses. Taken as isolated systems, chaotic dynamics appears to offer many impediments to anyone attempting to put them to use. The main problem to be addressed is then how to synchronize chaotic circuits. It is well known that two identical circuits are able to offer similar chaotic outputs. But if these circuits are not synchronized their output signals are not valid to be employed in a communication system. The main reason is the strong dependence of the obtained chaos on the initial and bounda ry conditions of the chaos generator circuit. Two chaotic signals with the same characteristics may have different values at any particular time if they are generated independently. Some additional conditions have to be imposed to the system in order to ob tain identical chaotic signals at any time. One of these conditions is the synchronization.

Several attempts have been made in this direction. The idea that chaotic systems could synchronize was first put forth in a paper almost ten years ago[1]. Several authors have followed the lines indicated in that paper. Pecora and Carroll[2-4] demonstrated the possibility of synchronizing chaotic subsystems with a common driving signal. Their idea was to decompose the chaotic dynamical system in two subsystems, "driving" and response" subsystems. The driving subsystem is composed by two state variable components whereas the second one just has one and uses as input signal one of the state components of the first subsystem. Several authors have followed this idea and sche mes using Chua's circuits are reported in the literature[5].

Another additional point needs to be considered. It concerns the characteristics of the chaotic signal to be employed. Almost in any of the reported situations the obtained chaos is analog. Although all physical systems are reall analog, communication and computer systems are nowadays digital ones. The way to use analog signals in digital systems in to make the conversion analog/digital. This idea has been employed in any case where an application to communication is needed. It should be useful to obtain digital chaos from the very beginning of the process and to employ it with the same requirements of the information signals.

The purpose of this paper is to present a way to obtain digital chaos a nd how to synchronize two chaotic systems. The main scheme of the proposed system is shown in Fig. 1. Two identical chaos generators, A and B, are located at emitte and receiver. Information signal is added at the receiver and transmitted to the network. This composed signal is detected at the receiver and processed with another chaotic signal obtained there. The resulting signal is the information generated at

* Correspondence: Email agonmar@tfo.upm.es; E.T.S. Ingenieros de Telecomunicación. Universidad Politécnica de Madrid, Ciudad Universitaria. 28040 Madrid. Spain

Photonic Devices and Algorithms for Computing III, Khan M. Iftekharuddin, Abdul Ahad S. Awwal, Editors, Proceedings of SPIE Vol. 4470 (2001) © 2001 SPIE · 0277-786X/01/$15.00

the emitter. This configuration is the basis of our system. The synchronization of two chaos gen erators is one of the main problems present when chaos is the intended method to encrypt a signal.

The present paper will show how the modulation must be performed at the emitter and how the demodulation must be accomplished at the receiver, in order to encrypt the information the carrier. A control to impose the same boundary and initial conditions at emitter and receiver is added to the emitter. The main blocks of the system are represented in Fig. 1.

One of the main problems concerns the type of signal to be transmitted. The problem should be easier if a multilevel signal should be taken. But in our case, just digital binary signals have been allowed. An analysis of the involved signals will be reported. The main consequences will be the characterizatio n of chaotic signals with and without an information signal added. This characterization will be performed with a fractal-like diagram corresponding to a particular phase diagram proposed by us. Binary data are transferred to hexadecimal values and these values are the basis to the phase diagram. Some other possible representations have been proposed too.

2. OPTICAL PROGRAMMABLE LOGIC CELL (OPLC)

The main block of our chaos generator is an Optically Programmable Logic Cell employed previously by us as a part of a possible optical compute [6]. Although this structure has been reported in several places[7-8], some of its principal characteristics will be here presented again. Its main characteristic is the logic processing of two input binary signals, governed by two control signals. Two outputs give logical functions of these inputs. The type of processing is related to the eight main Boolean Functions, namely, AND, OR, XOR, NAND, NOR, XNOR, ON and OFF. The programmable ability of the two outputs, as it has been described, allows the generation of several data coding for optical transmission. Moreover, as it was shown, this circuit has the possibility to the generation of periodic and even chaotic solutions. A precise analysis of the output characteristic versus the main variable parameters, as control signal level and data signal level, has been reported.

With this configuration, the above-mentioned digital character of the signal is directly obtained. Its main blocks are shown in Fig. 1. Two devices with a non-linear behaviour, P and Q, compose the circuit. The outputs of each one of them correspond to the two final outputs, O_1 and O_2, of the cell. Four are the possible inputs to the circuit. Two of them are fo input data, I_1 e I_2, and the other two, g and h, for control signals. The way these four inputs are arranged inside the circuit is also represented in Figure 1. A practical implementation we have carried out of the processing element has been based on an optoelectronical configuration. Lines in Fig. 1 rep esent optical multimode fibers. The indicated blocks, placed in order to

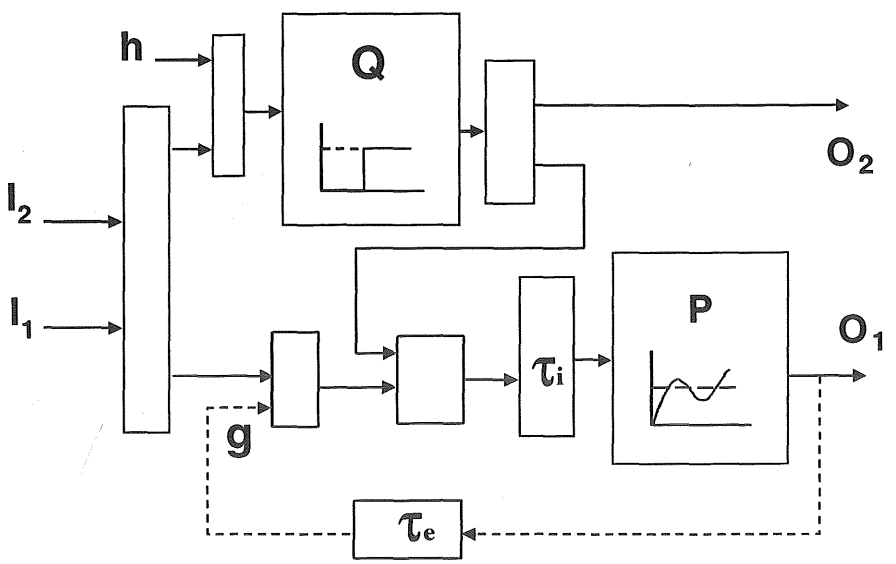

Fig. 1.- General structure of the Optically Programmable Logic Cell with feedback.

combine the corresponding signals, are conventional optical couplers. In this way, optical inputs arriving to the individual

devices are multilevel signals. The characteristics of the non-linear devices are also shown in Fig. 1. Device Q, corresponds to a thresholding or switching device, and device P is a multistate device, being the response of this non -linear optical device the one represented in Fig. 1. This response is similar to the behaviour of a SEED device. A feedback is drawn. It will be employed in the next use of this structure.

3. CHAOS GENERATION FROM AN OPLC

A non-linear behaviour is expected if some kind of feedback is applied to this cell. The feedback we have applied to the system, among the different possibilities, is the one going from the output O_1 of Q-device (see Fig. 1) to the control input, *g*, of P-device. No other additional control signal has been used. A chaotic output is obtained when the internal response time is made equal to zero or is much smaller than the external one. We have reported some results[9-12]. Some of them will be reviewed here in order to give some information for next paragraphs.

In order to study the non-linear response of our circuit, some minor modifications were performed. The first one was to introduce a feedback from one of the two possible outputs to one or both of the cell inputs. Moreover, according to previous studies in this field, the introduced feedback has to have some time delay. In the same way, because the results we are going to get will be obtained by computer simulation, another internal delay was needed. It corresponds to the real

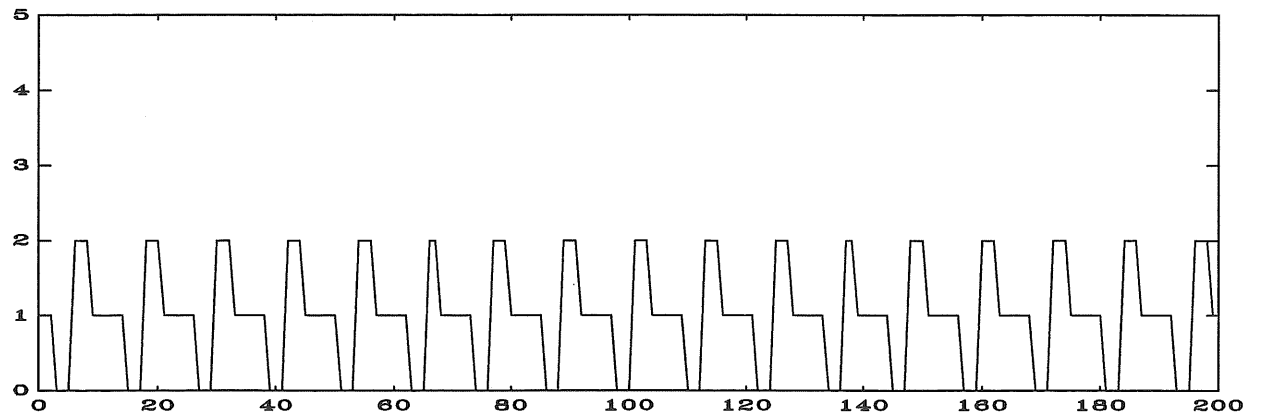

Fig. 2.- Input to the P device before feedback.

response time of the simulated nonlinear devices, **P** and **Q**.

In general, a periodic behaviour should be expected as the normal output of the system. But, under some conditions, this is not always true: the output is not periodic with some parameters values of the system.

The feedback applied to the system, among the different possibilities, is t he one corresponding from the output O_1

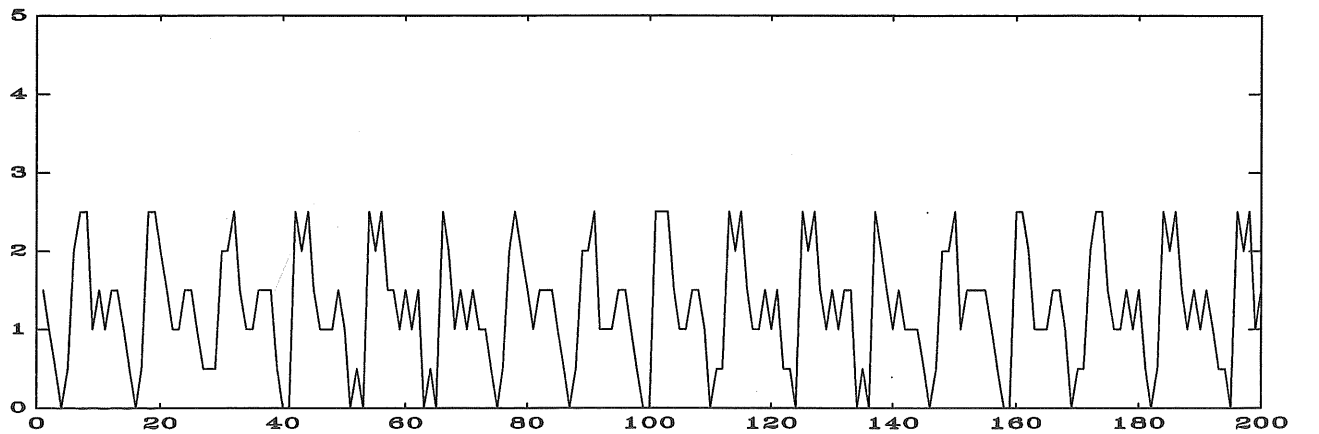

Fig. 3.- Input to the P device: feedback plus input signals.

of Q-device (see Fig. 1) to the control input, ***g***, of P-device. No other additional control signal has been used. Fig. 2 shows the final circuit with feedback.

According to previous studies[9-12], the situation with more probability to give a periodic or even chaotic solution is when internal delay time is shorter than the external one. In every one of our studied cases, a regular train of pulses has been the input. The real input to the device P, before the feedback takes place, is shown in Fig. 2. As it can be seen, it is a multilevel signal corresponding to the addition of the two inputs. The period of this signal, in this particular case, corresponds to a time of 14 bits.

If the ratio between internal and external delay times is smaller than 1, we obtain a periodic situation. Some examples are given in references[9-11]. But a chaotic output is obtained when the internal response time equal to zero or much smaller than the external one. Input signal, corresponding to feedback plus input data, to P-device control gate, is shown in Figure 3. Some output signals are given in [11]. No indication of a possible periodic behaviour has been obtained and, as it has been shown, it shows chaotic properties.

The main problem with the data we have is the way to extract some information from them. That means, how to operate with our digital signal where just two values, "0" and "1", are present. If we adopt just this output as possible values for a phase diagram representation, the resulting plot at the phase space should be concentrated on just four points, namely, (0,0), (0,1), (1,0) and (1,1). No information could be obtained from it. Hence a new technique has to be implemented.

The method we have adopted is to group sets of four consecutive bits and to convert them to their corresponding hexadecimal values. Hence, a sequence of zeroes and ones is converted to a new string of hexadecimal values, namely, 0, 1, and 2 up to 15. For example, "0010" would be a "2", "1001" a "9" and "1110" a "14". Four divides the total number of data, but much more information can be obtained from them than with simple binary signals. A diagram, similar to the t_{i+1} versus t_i in analogue signals, can be drawn in this way. In the case of periodic signals, a closed configuration is obtained. But in the case of chaotic signals, no definite pattern would be obtained. This situation appears in Fig. 4, where the plot for the output chaotic signal is shown.

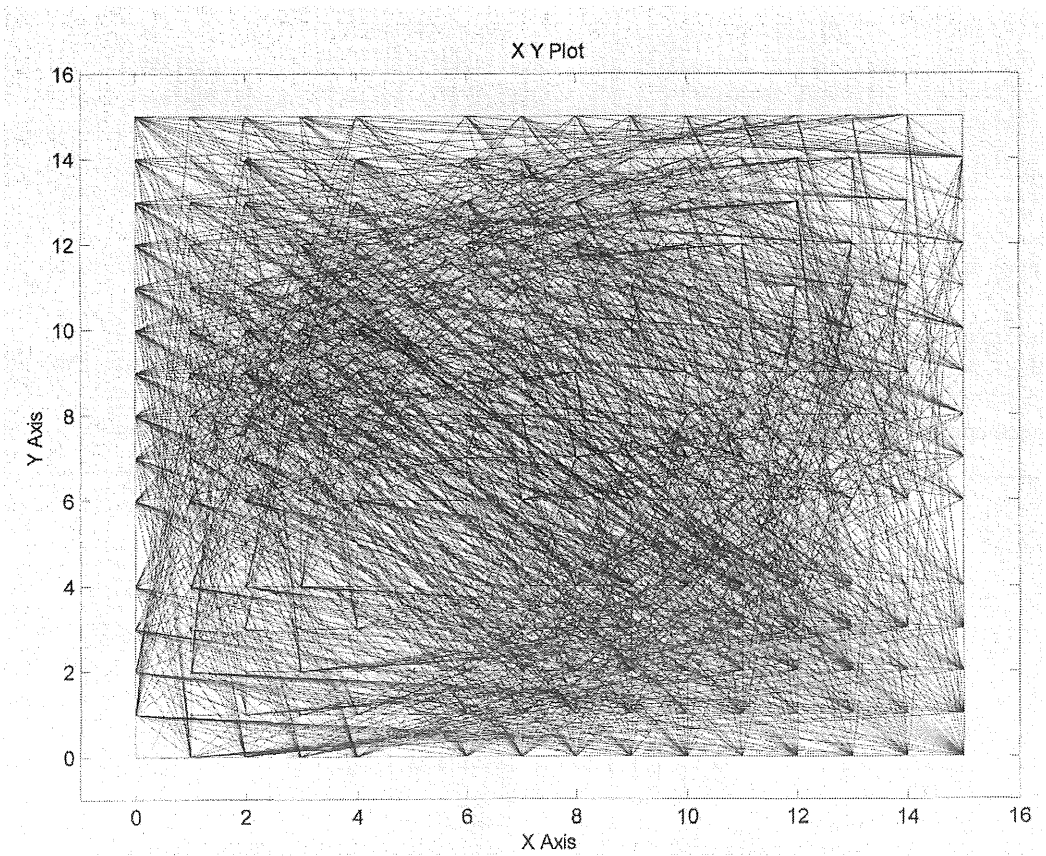

Figure 4.- Phase Diagram of Digital Chaos Signal.

The above phase diagram gives some ideas about the characteristics of the resulting signal. It is possible to know if the signal is periodic or has an irregular behaviour. Under certain circumstances it is possible to infer if it may have some

chaotic characteristics. But to really characterize the signals it is necessary to obtain some numerical information. We have obtained this with the help of the Lempel and Ziv complexity measure. We have presented this method and some results will be reported here because they will useful for our present work.[10].

The aim of the Lempel and Ziv method, as proposed by us, is to obtain some information about the characteristics of a long train of bits. The measure method introduced by the LZ algorithm was to associate the string complexity with the number of needed substrings to generate the initial string. Moreover, it is related too with the number of different substrings that have appeared and its apparition rate. The application of this method to a whole train of bits is very computer time consuming. It is useful when it is necessary to obtain the complete properties of the obtained string but under some circumstances a first approach, giving a general idea about the complexity of the signal, may be enough. This is the situation at our present work. It is because that we have worked with a string of 11500 data and divided it in substrings with 25 or 50 data. This is needed in order to allow an adequate charge to the computer. The first obtained result that may be seen wit more detail after cutting the digital signal in groups of 25 appears in Fig. 5. The number that appears in abscises is the order of the taken group. It is possible to see that the result changes from a group to the following one. The resulting graph indicates that there is an initial time, namely the corresponding to the first 50 groups, that the obtained values go from lo values for the relative complexity to values approaching the unity. The unity should correspond to a train of pulses with total random characteristics. This is an indication that the chaos generator needs a certain time interval to get the final state. This is a very important result to be applied in our present work. A similar result is obtained grouping bits in sets of 50 bits.

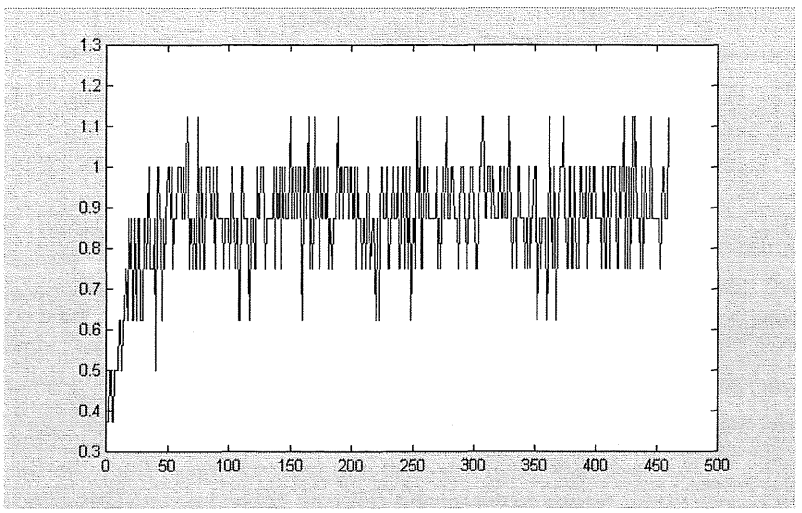

Fig. 5.- Analysis of a string with 11500 data bits grouped in packets of 25 bits.

In this case, the time to achieve a situation with complexity approaching the unity is shorter than in the previous case. This method will be adopted by in the following paragraphs to synchronize two chaos generators.

4. SYNCHRONIZATION OF CHAOTIC OPLCs

If two identical cells with feedback, as the above-mentioned, are parallel connected (Fig. 6) and the same signal arrives to their inputs, an identical chaos is obtained at their outputs. This situation corresponds to two identical and ideal configurations working under identical conditions. We have presented[12] these results previously. In order to recover the information signal, sent together with the chaos, an identical chaos must be subtracted from the incoming signal to the receiver. This is another problem when dealing with binary signals.

The behaviour becomes critical when the simulation tries to be close to a real situation. In this case, if both systems are not feed by exactly the same signal, the obtained outputs, although chaotic, are different. Hence, no possible relation between then should be feasible.

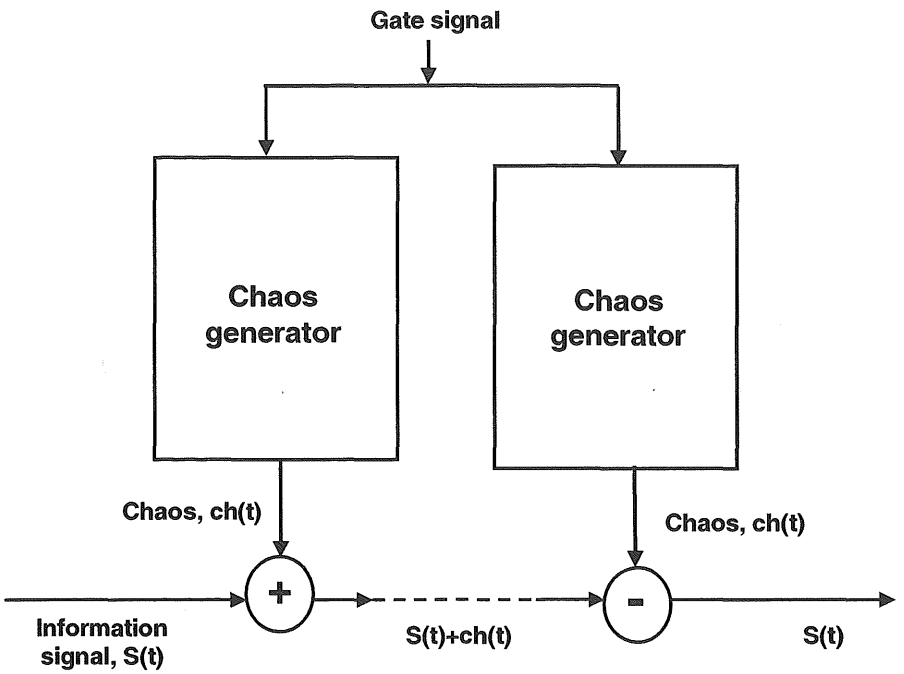

Fig. 6.- General structure for chaos synchronization in two chaos generators.

In a general situation, both systems, emitter and receiver, are located at different places. As a consequence, there is no possibility to introduce exactly the same input signals to thei corresponding input ports. This is because although a common signal generator could send the same train of pulses to both cells, the arriving times to them can be different. The time need to get the first cell is known if this generator is at the receiver place. But t he time when the signal arrives to the second cell may not be known. This is the most general case. Several solutions could be implemented to overcome this fact. We have presented some possible solutions to this problem previousl [12].

The solution adopted in the present case is shown in Fig. 7. Emitter and receiver are equipped with OPLCs able to generate chaotic signals. Both cells have identical characteristics and, hence, they can give rise to identical type of chaos. As it was pointed out before, the mai n problem is how to synchronize both systems.

Both systems initiate their operation by a pulse. This pulse may be sent from outside both systems or may be generated internally to any one of them. In any case, this signal initiates the generation of a multilevel signal, with equal characteristics in emitter and receiver. This signal is needed during the whole operation of the transmission and is, in a certain way, something like the signal bias for both optically programmable logic cells. Details about the characteristics of this signal have been published elsewhere. Because the OPLCs are feedbacked, both are able to generate a chaotic signal if internal conditions are the adequate.

The signals generated by both OPLCs go to Lempel and Ziv complexity measure systems able to give indication about the characteristics of the signal. As it was pointed out before, this type of chaos generator needs a certain amount of time to reach a situation close to chaos (Fig. 5).

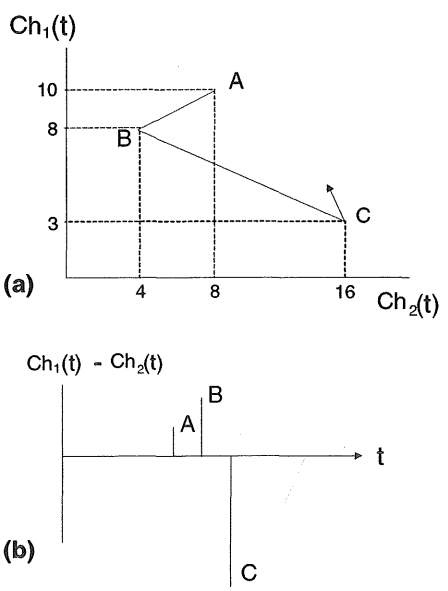

Fig. 8.- Methods employed to compare chaos signals. a) With hexadecimal data. b) By subtraction of chaos signals.

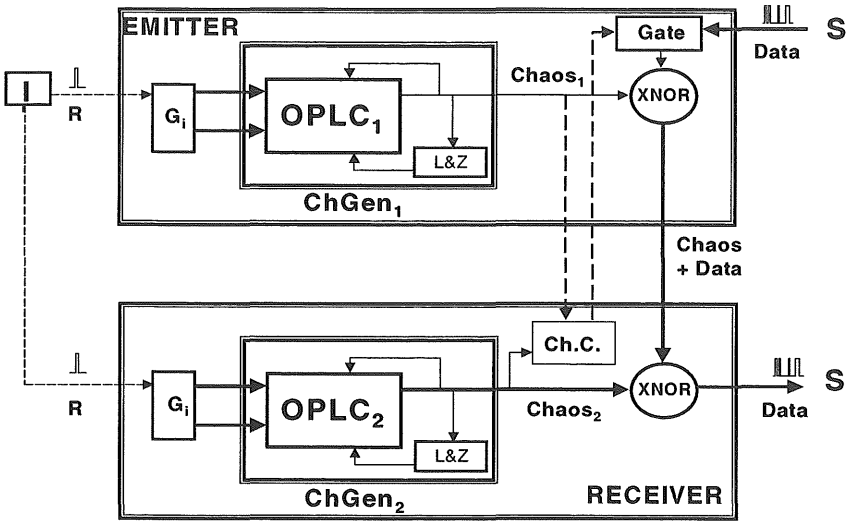

Fig. 7.- General structure of the communications system with chaotic synchronization in emitter and receiver.

When the obtained number approaches to the unity, a second circuit initiates its operation. It is the one designed as chaos comparator in Fig. 7.

Two methods have been implemented in order to know if both chaotic signals are exactly the same. The first one is shown in Fig. 8.a. Chaos signal from OPLC1 is represented at the x-axis and the one from OPLC2 at the y-axis. A hexadecimal representation, as before, was taken. The value of a particular case, when both signals are different, is represented in Fig. 9. This representation is performed for consecutive intervals of time. When both signals are the same one, the represented

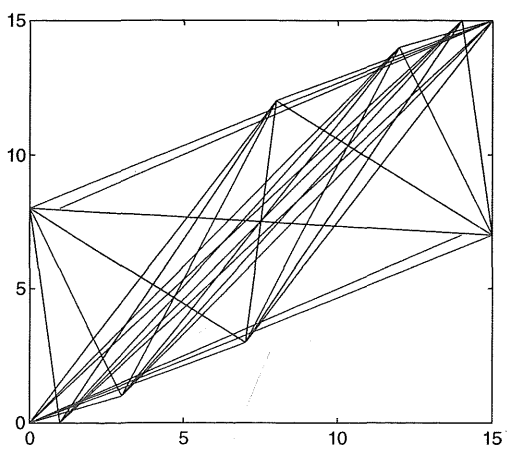

Fig. 9.- Application of method of fig. 8.a)

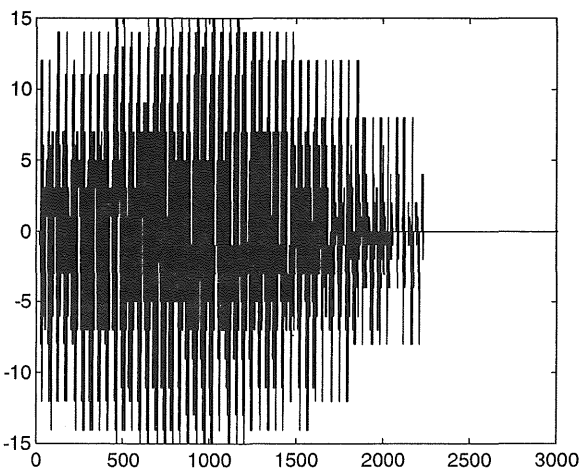

Fig. 10.- Subtraction of chaos signal from emitter and receiver. After a time period it can be seen that synchronizing is achieved.

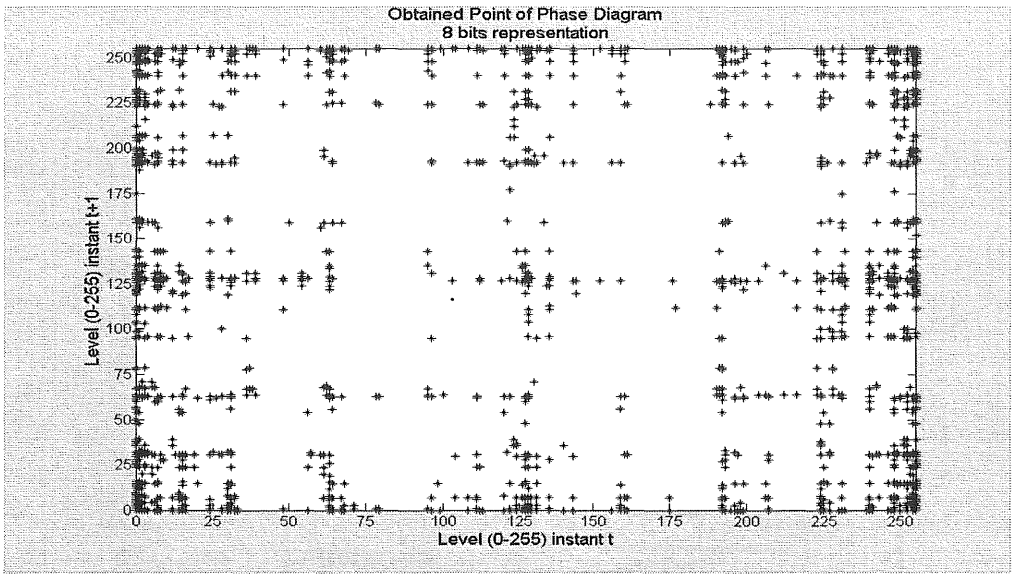

Fig. 11.- Obtained points in the Phase diagram of a chaotic signal with 256 reference levels

trajectory is a straight line going from point (0, 0) to point (15, 15). The system detects the line.

The second method represents the difference "Chaos from $OPLC_1$ – Chaos from $OPLC_2$" versus time. An example i given at Fig. 8.b. A final result, for a particular case, is shown in Fig. 10. It shows "Chaos from OPLC1 minus chaos from OPLC2" versus time. As it can be seen, after a certain number of steps, when synchronization is obtained, a horizontal line indicates this fact.

One of the main problems in any system like this one lies in the fact that emitter and receiver are not located at the same physical position. Due to that fact, there is delay time between the instant the signal was sent by the emitter and the reception time. Because chaos characteristics change with time, it is necessary to allow a certain control to analyze the situation at each instant. The block indicated as "chaos control" performs this operation.

Finall , in order to get an idea about the influence of the characteristics of the obtained signals when there is a certain

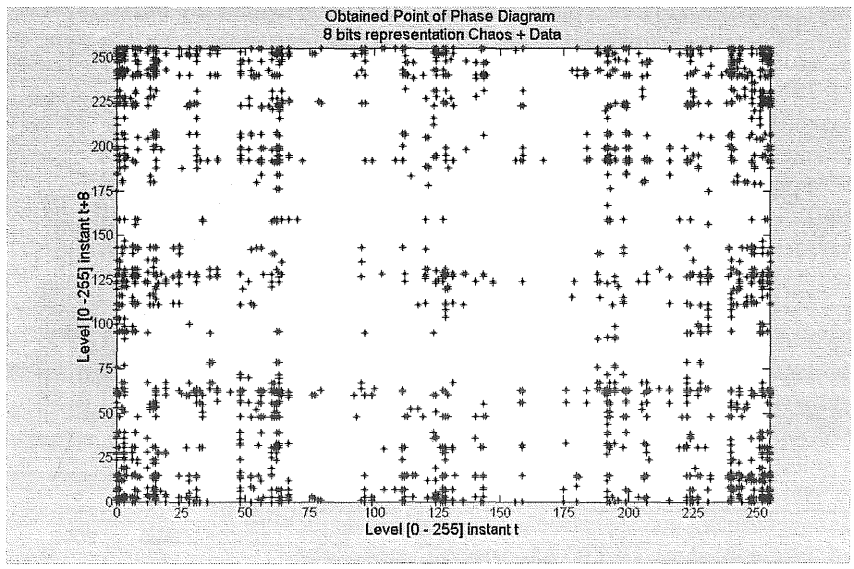

Fig. 02.-Obtained points in the Phase diagram of a chaotic signal plus data with 256 reference levels

data signal added to the chaotic signal, we have studied the influence of this fact on some of the above reported analysis tools. We have represented the chaotic signal in a phase diagram as we have done before but now we have extended the number of

levels to 256 instead the previous 16 levels. Moreover, we have not represented trajectories but just the initial and final points of each path. This new representation appears in Fig. 11. The number of represented points is 200000. If a simila representation to this one is performed for chaos signal plus a data signal, the result appears in Fig. 12. Itmay be seen that ther is not a clear difference between both figures. Hence, it is not possible from a representation as this one to infer the presence of information signals or not.

Fig. 13 shows the block diagram used to obtain last data simulation.

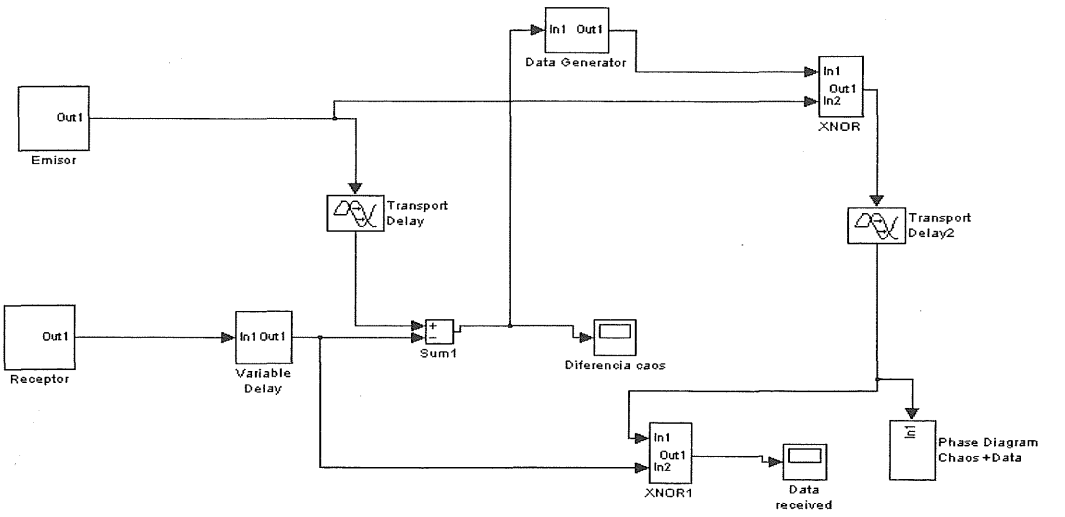

Fig. 13 .- Block diagram for data simulation on communication

5. CONCLUSIONS

A new method to synchronize chaotic circuits has been reported. The method is based on the use of Optically Programmable Logic Cells as chaos generators. Although these cells have been studied previously, some further studies are needed in orde to determine the characteristics of the obtained chaos when the initial driving signal changes. In this case, anew element has been introduced in the system. It analyses the chaos characteristics with the help of the Lempel and Ziv measure technique. It gives an indication about the complexity of the signal and, as a consequence, its chaotic characteristics. The de pendence with its parameters deserves also a deeper study. A study of how small and continuous changes affect the results is needed. Moreover, the influence of the presence of data in the chaotic signal is not clearly identified in a phase diagram.

ACKNOWLEDGMENTS

This work was partly supported by CICYT "Comisión Interministerial de Ciencia y Tecnología", grant TIC99 -1131 and CAM "Comunidad Autónoma de Madrid", grant 07T/0037/2000.

REFERENCES

1. V.S. Afraimovich, N.N. Verichev and M.I. Rabinovich, "St chastic synchronization of oscillations in dissipative systems", Inv. VUZ. Rasiofiz. RPQAEC **29**, 795-803, 1986.
2. L.M. Pecora and T.L. Carroll, "Synchronization in Chaotic Systems", Physical Review Letters **64**, 821, 1990.

3. L.M. Pecora, "Overview of Chaos and Communications Research". in "*Chaos in Communications*", **SPIE** Proceedings, 2038, 2-25, SPIE. Bellingham, WA. 1993.
4. T.L. Carroll and L.M. Pecora, "Synchronizing Chaotic Circuits", *IEEE Trans. on Circuits and Systems,* **38**, 453, 1991.
5. Several examples are given in "*Chua's Circuit: A Paradigm for Chao* ". Ed.: R.N. Madan. World Scientific Series on Nonlinear Science. World Scientific. London. 1993.
6. A. González-Marcos and J.A. Martín-Pereda, "Digital Chaotic Output from an Opticall -Processing Element", *Optical Engineering* **35**, pp. 525-535, 1996.
7. A. González-Marcos and J.A. Martín-Pereda, "Chaotic behaviour evaluation in optical logic gates with fractal concepts". Photonic Devices and Algorithms for Computing., *SPIE*, vol.3805, pp. 2-10, (1999).
8. A. González-Marcos & J.A. Martí -Pereda, "Analysis of irregular behaviour on an optical computing logic cell". Optics & Laser Technology, 32, 45557 – 466 (2000)
9. A. González-Marcos and J.A. Martín-Pereda, "Chaos synchronization in Optically Programmable Logic Cells ". Applications of Photonics Technology 3. Closing the Gap between Theory, Development, and Applications. Edited b G.A.Lampropoulos and R.A. Lessard. *SPIE*, vol. 3491, 340-345, (1998).
10. J.A. Martin-Pereda and A. Gonzalez-Marcos, "Analysis of digital chaotic optical signals", paper 4475-11. SPIE's 46th Annual Meeting. San Diego, California, USA (2001)
11. A. González-Marcos and J.A. Martín-Pereda, "Transmission of digital chaotic and information-bearing signals in optical communication systems". Mathematics of Data/Image Coding, Compression and Encryption II, SPIE , vol.3814, pp.36-42, (1999).
12. A. González-Marcos & J.A. Martín-Pereda, "*Digital Chaos Synchronization In Optical Networks*" . In "OPTICAL NETWORK DESIGN AND MODELLING II". Eds.: G. de Marchis y R.Sabella. Kluwer Academi Publishers, pp. 175-186. 1999.